**Invasão de conta da Apple revele fraca segurança**

A invasão da conta iCloud de um jornalista serve como alerta sobre o quão vulneráveis podem estar as pessoas em relação às ações de hackers mal-intencionados, não importando o quão digitalmente sofisticadas sejam as vítimas. Mat Honan, experiente jornalista de tecnologia, foi espetacularmente hackeado neste fim de semana.

Na noite de sexta-feira, a senha da conta iCloud de Honan foi alterada. Mais tarde, os bandidos invadiram sua conta Gmail, e, logo em seguida, apagaram os dados em seu iPad, iPhone e MacBook Air usando o recurso de apagamento remoto da Apple — um mecanismo de autodestruição projetado para uso quando um dispositivo cair em mãos erradas. Para piorar a situação, eles também acessaram sua conta pessoal no Twitter, bem como a conta pertencente ao blog de tecnologia Gizmodo, onde ele costumava trabalhar.

Honan ainda tem que contar a história completa. Mas diz ele que os hackers conseguiram entrar após contatar por telefone o suporte técnico da Apple e usar alguma tática inteligente de “engenharia social” para evitar perguntas de confirmação de identidade. Isso pode apontar para uma fraqueza no processo de verificação de identidade da Apple.

Mas a raiz do problema pode ser o fato da Apple incentivar seus clientes a usar a mesma senha de seu Apple ID para quase tudo. Essa é uma preocupação porque o iTunes não é mais apenas uma loja de música, é também um lugar para comprar e-books, aplicativos e programas de TV. E as mesmas credenciais são usadas para fazer login no iCloud, serviço de nuvem da Apple, onde documentos confidenciais podem ser armazenados ou um apagamento remoto de dados pode ser executado, como se deu no caso de Honan.

“A Apple quer fingir que tudo é magia”, disse Alex Stamos, cofundador da iSEC Partners, uma firma de segurança. “Eles precisam admitir que seus produtos podem ser usados por pessoas malvadas com propósitos malignos”.

Um problema, disse Stamos, é que os clientes do iTunes usam uma única conta e senha para acessar todos os serviços da Apple. Por exemplo, o mesmo login pode ser usado para baixar um jogo de US$ 1 ou comprar um laptop de US$ 2.000 na loja on-line da Apple. Ele disse que a empresa poderia adotar um método de verificação em dois passos como o do Google. Por exemplo, se um usuário quiser fazer login na loja iTunes em um novo dispositivo, a Apple poderia enviar uma mensagem para o tal aparelho com um código que o usuário precisaria digitar de modo a verificar sua identidade.

Justiça seja feita: o iTunes é bem-sucedido em grande parte porque foi um dos primeiros sistemas “sem atrito” que permitia comprar conteúdo digital. Mas talvez tenha se tornado grande demais e poderoso demais para continuar sendo tão simples.

Link: <http://oglobo.globo.com/sociedade/tecnologia/invasao-de-conta-da-apple-revela-fraca-seguranca-5703490#ixzz3Zm0pQH3j>

**Em entrevista, Tim Cook fala sobre a invasão de contas do iCloud (Apple).**

Essa história já teve três partes: a primeira envolveu fotos de celebridades nuas que vazaram — sabemos que ao menos algumas estavam armazenadas no iCloud; na segunda, tivemos a declaração da Apple afirmando que o iCloud está seguro e que roubo das fotos de celebridades foi um “ataque direcionado”; já na terceira, vimos que a verificação em duas etapas não protege totalmente usuários do serviço na nuvem da Maçã. Pois agora estamos no quarto ato: uma entrevista do CEO da Apple explicando o que houve e o que a empresa pretende fazer daqui para frente.

Ao Wall Street Journal, **Tim Cook** afirmou que as contas do iCloud foram invadidas pois crackers conseguiram responder corretamente as perguntas de segurança ou tiveram êxito em ataques de phishing — em ambos os casos, ganhando acesso às senhas das contas.

Para melhorar esse sistema, Cook disse que sua empresa irá alertar usuários via email e através de notificaçõespush quando alguém tenta alterar a senha da conta, restaurar os dados do iCloud para um novo dispositivo ou quando uma determinada conta for registrada pela primeira vez num dispositivo. Atualmente, usuários já são alertados por email quando alguém tenta mudar a senha ou se conectar pela primeira vez a partir de um dispositivo desconhecido.

Essas mudanças deverão ser colocadas em prática em até duas semanas. O CEO disse ainda que o novo sistema permitirá que usuários tomem medidas imediatas como alterar a senha para retomar o controle da conta ou alertando a equipe de segurança da Apple.

Mais do que a parte técnica, Cook acha que a Apple poderia ter feito mais em prol de usuários, deixando claro o quão importante é criar senhas fortes e da ativação do sistema de verificação em duas etapas. Por falar nele, o CEO disse que a maioria dos usuários não utiliza esse sistema de proteção e que planeja estimular a ativação dele de forma mais agressiva.

Se as celebridades tivessem o sistema [de verificação em duas etapas] ativado, os hackers não teriam tido a oportunidade de adivinhar a resposta correta para as questões de segurança.

Segurança nunca é demais. Contudo, eu não consegui entender exatamente como essas mensagens (por email e notificações push) ajudarão usuários. Nesse ponto eu concordo 100% com Ashkan Soltani, pesquisador de segurança independente que foi consultado pelo WSJ. De acordo com ele, as notificações farão pouco para proteger os consumidores já que os alertas são disparados quando tudo já está acontecendo — ou seja, quando o roubo da senha já está sendo colocado em prática.

Vamos torcer para que a Apple faça mais do que simplesmente disparar esses alertas e encorajar o uso da verificação em duas etapas.

Link: <https://macmagazine.com.br/2014/09/05/em-entrevista-tim-cook-fala-sobre-a-invasao-de-contas-do-icloud/>

**Hackers afirmam ter encontrado um jeito fácil de invadir contas do iCloud.**

Logo no início de 2015, a Apple pode estar prestes a reviver uma das maiores crises que enfrentou durante o ano passado. Tudo isso graças ao grupo hacker Pr0x13, que lançou no GitHub uma ferramenta batizada como iDict — que supostamente é capaz de pular restrições e processos de autenticação de qualquer conta do iCloud.

Segundo os responsáveis pelo software, sua criação só se tornou possível graças a um bug “dolorosamente óbvio” do sistema da Apple descoberto há um tempo considerável. O grupo afirma que não vai se responsabilizar pela forma como as pessoas vão usar o aplicativo, convidando consumidores a relatar o problema à companhia para que ela possa corrigi-lo rapidamente.

Caso o iDict seja tão eficiente e fácil de usar quanto o afirmado pelo Pr0X13, isso pode levar a uma repetição do escândalo que resultou na divulgação de fotos íntimas de celebridades em 2014. Para evitar uma situação do tipo, a Apple precisa agir rapidamente para corrigir o problema — segundo usuários do Twitter e alguns Redditors, a ferramenta funciona conforme o prometido, o que significa que a divulgação de informações confidenciais é somente questão de tempo.

Link: <http://www.tecmundo.com.br/apple/70909-hackers-afirmam-ter-encontrado-jeito-facil-invadir-contas-icloud.htm>

**Apple responde ao problema da invasão da conta iCloud de um jornalista: “Vamos melhorar a segurança”.**

O caso que aconteceu no último final de semana serviu de alerta para a Apple e todos os serviços de nuvem, além dos próprios usuários. Após um jornalista ter tido a sua conta iCloud invadida e todos os seus dados pessoais apagados, iniciou-se uma investigação para entender como os criminosos conseguiram tal façanha, chegando-se a conclusões importantes que envolvem Apple e Amazon. E o próprio jornalista assume: “Foi um pouco culpa minha, isto poderia ter sido evitado“.

Para Mat Honan, a vítima da invasão, o grande problema é que ele sempre teve todas as suas contas interligadas umas às outras. Apple ID interligada com conta do Gmail, que era associada à conta do **Twitter**, que no final das contas, era o objetivo final dos criminosos, para publicar mensagens racistas e homofóbicas. E isso poderia ter sido evitado se ele tivesse adotado a verificação em duas etapas do Google.

Mas como os invasores conseguiram que os técnicos da AppleCare fornecessem acesso à conta de Mat, pelo telefone?

A Apple faz algumas perguntas de segurança para se certificar de que a pessoa é mesmo quem diz que é. São elas:

* Endereço onde mora
* O endereço eletrônico @me da pessoa
* Os 4 últimos números do cartão de crédito associado à conta

O endereço pode ser facilmente conseguido procurando nos registros de domínio do jornalista. Infelizmente esta informação é exposta para todos na maioria dos provedores. O endereço @me foi conseguido na página de recuperação de senha do Google, e os números do cartão de crédito, pela conta da **Amazon**. A mesma informação que para a Apple é importante, a Amazon acha trivial, expondo os 4 últimos números do cartão para todo mundo ver. E foi assim que eles fizeram: descobriram primeiro as informações vitais e depois ligaram para a Apple, se fazendo passar pelo jornalista.

A partir daí, não foi difícil ter acesso aos outros serviços, pois todos estavam interligados.

A Apple emitiu um comunicado oficial sobre o caso:

A Apple leva a sério a privacidade dos usuários e requer múltiplas formas de verificação antes de redefinir uma senha de ID da Apple. Neste caso específico, os dados do cliente foram comprometidos por uma pessoa que havia adquirido as informações pessoais sobre o cliente. Além disso, descobrimos que as nossas próprias políticas internas não estavam sendo completamente seguidas. Estamos revendo todos os nossos processos para redefinir senhas de conta para garantir que os dados de nossos clientes sejam protegidos.

O caso revelou diversas brechas de segurança entre os serviços de internet. Um serviço deixa vazar informações que são importantes para outro, e vice-versa, permitindo que se faça uma “engenharia social” para se descobrir senhas e informações pessoais de qualquer um. O que aconteceu pode ter sido terrível para a vida pessoal do jornalista (que perdeu para sempre um ano de fotos da sua filha), mas foi muito importante para que os atuais serviços de nuvem melhorem ainda mais a segurança dos dados.

O mundo moderno se dirige para a transferência para as nuvens (clouds). A Apple está investindo pesado no iCloud, o Google e a Amazon têm **tudo** na nuvem e a Microsoft também está tomando o mesmo caminho. Por isso, é inútil dar a culpa para os serviços de nuvem, pois eles parecem ser um caminho sem volta. O que temos que fazer é nos preocupar em manter nossos dados sempre seguros e com poucas brechas de segurança.

Algumas dicas de segurança:

* use sempre senhas com mais de 8 dígitos, que contenham números entre as letras (tipob10gdoiph0n3, ou coisa parecida). É um saco digitar isso sempre, mas é a certeza que sua conta está segura
* não associe sua conta da Apple para a recuperação de senhas em serviços externos, como Google, Yahoo, Hotmail e outros. Há quem sugira criar uma conta separada só para recuperação de senhas, que ninguém saiba o endereço.
* se você tem conta no Google, habilite a verificação em duas etapas
* faça sempre backup. Sempre.

Link: <http://blogdoiphone.com/2012/08/apple-responde-ao-problema-da-invasao-da-conta-icloud-de-um-jornalista-vamos-melhorar-a-seguranca/>